Journal of Universal Computer Science, vol. 15, no. 15 (2009), 2937-2956
submitted: 1/2/09, accepted: 29/8/09, appeared: 1/9/09 © J.UCS

Information Theoretically Secure Encryption with Almost Free Authentication

Basel Alomair
(Center of Excellence in Information Assurance (CoEIA)
King Saud University, Riyadh, Saudi Arabia
&
Network Security Lab (NSL)
University of Washington, Seattle, WA, USA
alomair@uw.edu)

Radha Poovendran
(Network Security Lab (NSL)
University of Washington, Seattle, WA, USA
rp3@u.washington.edu)

Abstract: In cryptology, secure channels enable the exchange of messages in a confidential and authenticated manner. The literature of cryptology is rich with proposals and analysis that address the secure communication over public (insecure) channels. In this work, we propose an information theoretically secure direction for the construction of secure channels. First, we propose a method of achieving unconditionally secure authentication with half the amount of key material required by traditional unconditionally secure message authentication codes (MACs). Key reduction is achieved by utilizing the special structure of the authenticated encryption system. That is, authentication exploits the secrecy of the message to reduce the key material required for authentication. After the description of our method, since key material is the most important concern in unconditionally secure authentication, given the message is encrypted with a perfectly secret one-time pad cipher, we extend our method to achieve unconditionally secure authentication with almost free key material. That is, we propose a method for unconditionally authenticating arbitrarily long messages with much shorter keys. Finally, we will show how the special structure of the authenticated encryption systems can be exploited to achieve provably secure authentication that is very efficient for the authentication of short messages.

Key Words: Unconditional security, authentication, encryption
Category: E.3, E.4, F.2, F.2.1, G.2, G.2.3

1 Introduction and Related Work

When a secret message is to be transmitted through a public channel, the message cannot be transmitted in clear text; otherwise, unauthorized receivers listening to the public channel can infer the communicated secret. Fortunately, however, the problem of communicating secretly over public channels has been studied extensively, with a variety of good solutions available. The literature of cryptography is rich with proposed ciphers that transform plaintext messages into ciphertexts for the purpose of making the illegitimate receivers' task of breaking the confidentiality of the transmitted messages more challenging. Of course, the level of secrecy that can be achieved by different ciphers varies according to their specifications. (Confidentiality and secrecy will be used synonymously in the paper.)

There are three main components in any cipher: a plaintext message to be communicated secretly, a ciphertext to be transmitted through the public channel, and a key that is used to transform the plaintext message into its corresponding ciphertext. The properties of the cipher that transforms plaintext messages into ciphertexts determine the level of secrecy that can be achieved. In his celebrated work, Shannon [Shannon(1949)] put forth the notion of perfect secrecy and derived the necessary conditions to achieve it. Shannon proved that only one class of ciphers can achieve perfect secrecy, namely one-time pad (OTP) ciphers (e.g., the well-known Vernam OTP cipher [Vernam(1926)]).

Confidentiality, however, is only one objective of security systems; integrity is another one. (Integrity and authenticity will be used interchangeably throughout the rest of the paper.) Therefore, in applications where adversaries can actively modify the transmitted message, encrypted messages are to be protected with mechanisms to ensure their integrity. A message authentication code (MAC) is a symmetric key cryptographic primitive designed specifically to ensure message integrity.

In authentication schemes, the term unconditional security is analogs to the term perfect secrecy in encryption scheme; they both imply security against computationally unbounded adversary.[1] The first unconditionally secure authentication codes were invented by Gilbert *et al.* in [Gilbert et al.(1974)Gilbert, MacWilliams and Sloane]. The use of universal hash functions for the purpose of designing unconditionally secure authentication codes was introduced by Wegman and Carter [Wegman and Carter(1979)]. In their scheme, let a' and b' be the lengths of the messages and their MACs, respectively. Let $s = b' + \log_2 \log_2 a'$. Given a strongly universal class of functions $\mathcal{H}$ that maps strings of lengths $2s$ into strings of lengths s, they constructed a small, almost universal class $\mathcal{H}'$. Each member of $\mathcal{H}'$ is constructed from a sequence of length $\log_2 a' - \log_2 b'$ members of $\mathcal{H}$. Let $(f_1, f_2, \cdots)$ be such sequence and let $f' = (f_1, f_2, \cdots)$. The message to be authenticated is broken into substrings of lengths $2s$; that is, a message of length a' will be divided into $\lceil \frac{a'}{2s} \rceil$ substrings of equal lengths. Now, f_1 is applied to all substrings and the results are concatenated to give a string of roughly half the length of the original message. This process is repeated with $f_2, f_3, \cdots$, until a substring of length s is reached. The MAC (the output of f') is the low-order b' bits of s. The key needed to specify f' is the concatenation of the keys needed to specify $f_1, f_2, \cdots$. For unconditional security to hold, the function f' cannot be used more than once. In [Wegman and Carter(1979)], however, the authors discussed an extension to which the same function can be used to authenticate multiple, but limited, number of messages.

[1] Information-theoretic security and unconditional secrecy will be used synonymously to mean perfect secrecy

In [Wegman and Carter(1981)], Wegman and Carter were the first to apply strongly universal hash families for message authentication. In unconditional authentication, since keys cannot be used for arbitrarily number of times, the amount of used key material is of particular importance. Stinson [Stinson(1994)] formally defined the notion of almost strongly universal hash families in order to reduce the key length required for unconditional authentication ([Stinson(1996)] is a good survey paper on unconditionally secure MACs). Much of the theory of unconditional authentication was developed by Simmons, who proved many fundamental results in the area [Simmons(1988)].

Universal hash families were also used for the design of computationally secure MACs, e.g., [Bernstein(2005), McGrew and Viega(2004), Halevi and Krawczyk(1997), Etzel et al.(1999)Etzel, Patel and Ramzan, Black et al.(1999)Black, Halevi, Krawczyk, Krovetz and Rogaway, Kaps et al.(2005)Kaps, Yuksel and Sunar]. Other computationally secure MACs include, but are not limited to, CBCMAC [US National Bureau of Standards(December 1980)], XORMAC [Bellare et al.(1995)Bellare, Guerin and Rogaway], HMAC [Bellare et al.(1996)Bellare, Canetti and Krawczyk], and PMAC [Rogaway and Black(2001)].

In this work, we address the problem of *authenticated encryption*. In authenticated encryption schemes, systems that combine message encryption and authentication are constructed. A generic approach to achieve authenticated encryption is to compose a system by combining an encryption scheme and an authentication scheme. There are three different approaches to construct generic authenticated encryption schemes, *encrypt and authenticate* ($E\&A$), *authenticate then encrypt* (AtE), and *encrypt then authenticate* (EtA). The transport layer of SSH uses a variant of $E\&A$ [Ylonen and Lonvick(2006)], SSL uses a variant of AtE [Freier et al.(1996)Freier, Karlton and Kocher], while IPSEC uses a variant of EtA [Kent(2005)]. Detailed discussions about generic constructions and their security relations can be found in [Bellare and Namprempre(2000), Krawczyk(2001)].

Dedicated authenticated encryption schemes, on the other hand, are the ones designed to achieve the two goals in one primitive, as opposed to combining two primitives as in generic constructions. Proposals that use simple checksum or manipulation detection code (MDC) have appeared in [Meyer and Matyas(1982), Kohl and Neuman(1993), Gligor and Donescu(2000)]. Such simple schemes, however, are known to be vulnerable to attacks [Jutla(2001)]. Other block ciphers that combine encryption and message authenticity include [Jutla(2001), Gligor and Donescu(2002), Rogaway et al.(2003)Rogaway, Bellare and Black, Ferguson et al.(2003)Ferguson, Whiting, Schneier, Kelsey, Lucks and Kohno, Kohno et al.(2004)Kohno, Viega and Whiting, Bellare et al.(2004)Bellare, Rogaway and Wagner].

In [Jutla(2001)], Jutla proposed the integrity aware parallelizable mode (IAPM), an encryption scheme with authentication. The authenticated encryption requires a total of $m + 2$ block cipher evaluation for a message of m blocks. Gligor and Donescu proposed the XECB-MAC [Gligor and Donescu(2002)]. Rogaway *et al.* [Rogaway et al.(2003)Rogaway, Bellare and Black] proposed OCB: a block-cipher mode of operation for efficient authenticated encryption. For a message of length M-bits and an n-bit cipher block size, their method requires $\lceil \frac{M}{n} \rceil + 2$ block cipher runs. For more on the literature of dedicated authenticated encryption schemes, interested readers may refer to [van Tilborg(2005)].

CONTRIBUTIONS. In this paper, we construct authenticated encryption schemes. The main objective of this work is to exploit the authenticated encryption structure to reduce the amount of key material required for unconditionally secure authentication. In the first proposed scheme, we utilize the fact that the message is encrypted with an information theoretically secure cipher to design an unconditionally secure MAC with half the amount of key material required by traditional methods. In the second scheme, we extend the first scheme to further reduce the amount of key material required for message authentication. The extended scheme allows for unconditional authentication of arbitrarily long messages with very short keys, thus, resulting in an almost free authentication. Finally, since traditional MACs can be inefficient when used to authenticate short messages, we describe an efficient method for authenticating short encrypted messages.

ORGANIZATION. The rest of the paper is organized as follows. Section 2 provides a detailed description of our security definitions and assumptions about the adversary's knowledge and resources, along with a list of used notations and the simple preliminaries about the finite ring $\mathbb{Z}_p$ that will be used for our security analysis. Section 3 is dedicated to describing the details of the proposed authenticated encryption scheme. The security analysis of the proposed scheme is provided in Section 4. In Section 5 we compare our scheme to existing techniques and discuss some examples of potential applications of our scheme. Section 6 details our extended approach that can reduce the amount of required key material. In Section 7, we describe our efficient, provably secure, method for authenticating short encrypted messages. We conclude our paper in Section 8.

2 Notations and Communication Model

In this section we state our assumptions and describe the notations and definitions that will be used for the rest of the paper.

2.1 Notations

The following notations will be used throughout the rest of the paper.

- For two sets $A \subset B$, we denote by $B \backslash A$ the set of elements in B that are not in A.
- For the set $\mathbb{Z}_p \stackrel{\text{def}}{=} \{0, 1, ..., p-1\}$, the set $\mathbb{Z}_p^*$ is defined to be the set of integers relatively prime (co-prime) to p. When p is a prime integer $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\} \stackrel{\text{def}}{=}$

$\{1, 2, ..., p-1\}$. For the rest of the paper, the two notations $\mathbb{Z}_p^*$ and $\mathbb{Z}_p \backslash \{0\}$ will be used interchangeably to emphasize the co-prime property or the exclusion of the zero element, respectively.

- For an integer n, the set $n\mathbb{Z}$ will denote the set of integers that are multiples of n.
- For any two strings a and b, $(a \mid\mid b)$ denotes the concatenation operation.
- For the rest of the paper, $(+)$ and $(\times)$ represent addition and multiplication over $\mathbb{Z}_p$, even if the $\pmod p$ part is dropped for simplicity.
- For any two integers a and b, $\gcd(a, b)$ is the greatest common divisor of a and b.
- For an element a in a ring R, the element a^{-1} denotes the multiplicative inverse of a in R, if it exists.
- Throughout the rest of the paper, random variables will be represented by bold font symbols, whereas the corresponding non-bold font symbols represent specific values that can be taken by these random variables.

2.2 Model Assumptions and Security Goals

Without loss of generality, we assume there is only one channel of communication that both legitimate users and the adversary share. More specifically, we assume the legitimate receiver and the adversary are listening to the same channel and the adversary has access to all bits transmitted in this channel. Furthermore, we assume the adversary has complete control over the communication channel. That is, we assume the adversary's ability to purposely flip transmitted bits at any position of her choice. Legitimate users are assumed to share a secret key that allows them to communicate secretly as long as this key has not been exposed.

The proposed cipher is designed to achieve two goals. The first goal is perfect secrecy in Shannon's information-theoretic sense. The cipher is information-theoretically secure if the ciphertext gives no information about the plaintext, i.e., the ciphertext and the plaintext are statistically independent. Formally, perfect secrecy is defined as:

Definition 1 Perfect Secrecy [Stinson(2006)]. *For a plaintext m and its corresponding ciphertext φ, the cipher is said to achieve perfect secrecy if* $\Pr(\boldsymbol{m} = m | \boldsymbol{\varphi} = \varphi) = \Pr(\boldsymbol{m} = m)$ *for all plaintext m and all ciphertext φ. That is, the a posteriori probability that the plaintext is m, given that the ciphertext φ is observed, is identical to the a priori probability that the plaintext is m.*

This definition implies that, given the ciphertext, a *computationally unbounded* adversary cannot do better than randomly guessing the plaintext. Throughout the rest of the paper, perfect secrecy, unconditional secrecy, and information-theoretic security will be used synonymously.

The second goal of our design is to provide message integrity by achieving resilience to active or message corruption attacks. To formally define resilience to active attacks we start with the definition of negligible functions.

Definition 2 Negligible Functions [Goldreich(2001)]. *A function $\gamma : \mathbb{N} \rightarrow \mathbb{R}$ is said to be negligible if for any nonzero polynomial p, there exists N_0 such that for all $N > N_0$, $|\gamma(N)| < \frac{1}{|p(N)|}$. That is, the function is said to be negligible if it converges to zero faster than the reciprocal of any polynomial function.*

In the sense of Definition 2, resilience to active attacks is defined as follows.

Definition 3 Resilience to Active Attacks [Aloamir and Poovendran(2009)]. *An authenticated encryption scheme is said to be resilient to active attacks if and only if the probability of legitimate receivers accepting a corrupted ciphertext is negligible.*

The cipher is said to provide message integrity if it is resilient to active attacks. Unconditionally secure MACs demands more than resilience to active attacks. Just like perfect secrecy, unconditionally secure authentication implies security against computationally unbounded adversaries.

2.3 Preliminaries

The security of the proposed cipher is based on unique properties of the finite integer ring $\mathbb{Z}_p$. Of course, in the special case where p is a prime integer, $\mathbb{Z}_p$ becomes a field. The integer field $\mathbb{Z}_p$ possesses unique properties that make it attractive in many applications in cryptography, such as the well-known El-Gamal public-key cryptosystem [Elgamal(1985)]. In this paper, we will introduce a new use of the field $\mathbb{Z}_p$ in symmetric-key cryptography. The properties of the field $\mathbb{Z}_p$ required to establish the security of our scheme are stated below as lemmas.

Lemma 4. *For a prime integer p, and any two integers α and β in $\mathbb{Z}_p$, if p divides $\alpha \times \beta$, then at least one of the integers α and β must be the zero element. Formally, if p is a prime integer, the following implication must hold.*

$$\{\ \alpha \times \beta \equiv 0 \pmod p\ \} \Rightarrow \{\ \alpha \equiv 0 \pmod p \ \text{ OR } \ \beta \equiv 0 \pmod p\} \tag{1}$$

Lemma 4 is basically a restatement of the fact that, for a prime integer p, the ring $\mathbb{Z}_p$ is an integral domain.

Lemma 5. *Let p be a prime integer. Then, given an integer $k \in \mathbb{Z}_p^*$, for an r uniformly distributed over $\mathbb{Z}_p$, the value δ given by:*

$$\delta \equiv r \times k \pmod p \tag{2}$$

is uniformly distributed over $\mathbb{Z}_p$.

Lemma 5 is a direct consequence of the fact that, for a prime integer p, the ring, $\mathbb{Z}_p$, is a filed.

In this paper, we use these lemmas in a novel way that has not been proposed in cryptographic literature.

3 An Unconditionally Secure Authenticated Encryption Scheme

In this section, we describe our basic unconditionally secure authenticated encryption scheme that requires half the key material required by traditional unconditionally secure MACs based on universal hash functions.

3.1 Cryptosystem

Let p be a prime integer that the legitimate users have pre-agreed upon based on required security performance. The security parameter, ℓ, is the length of p in bits. Let the legitimate users share a key $k = k_1||k_2$, where k_1 and k_2 are secret and chosen *independently* and *uniformly* from the sets $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively. We emphasize that k_1 and k_2 must be statistically independent.

For any nonzero message $m \in \mathbb{Z}_p \backslash \{0\}$, define two functions $\varphi_{k_1}(m) : \mathbb{Z}_p \backslash \{0\} \rightarrow \mathbb{Z}_p$ and $\varphi_{k_2}(m) : \mathbb{Z}_p \backslash \{0\} \rightarrow \mathbb{Z}_p^*$ as follows:

$$\varphi_{k_1}(m) \equiv k_1 + m \pmod p, \tag{3}$$

$$\varphi_{k_2}(m) \equiv k_2 \times m \pmod p. \tag{4}$$

As a function of the key, k, the ciphertext of the plaintext message, m, is the concatenation of $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$. That is,

$$\varphi_k(m) = \varphi_{k_1}(m) \;||\; \varphi_{k_2}(m). \tag{5}$$

(Equivalently, the exclusive-or operation can be used instead of the addition operation in equation (3) without affecting the cipher's security properties).

Upon receiving the ciphertext, $\varphi'_k(m)$, the receiver extracts a plaintext, m', as follows:

$$m' = \varphi'_{k_1}(m) - k_1 \pmod p. \tag{6}$$

The integrity of the extracted m' is verified by the following check:

$$m' \times k_2 \stackrel{?}{\equiv} \varphi'_{k_2}(m) \pmod p. \tag{7}$$

The notations $\varphi'_k(m)$ and m' are to reflect the possibility of receiving a modified ciphertext. The ciphertext is considered valid if and only if the integrity check of equation (7) is passed. Wherever is convenient, $\varphi_{k_2}(m)$ will be referred to as the MAC of m (since its purpose is to provide message integrity).

A block diagram to implement the proposed authenticated encryption scheme is depicted in Figure 1.

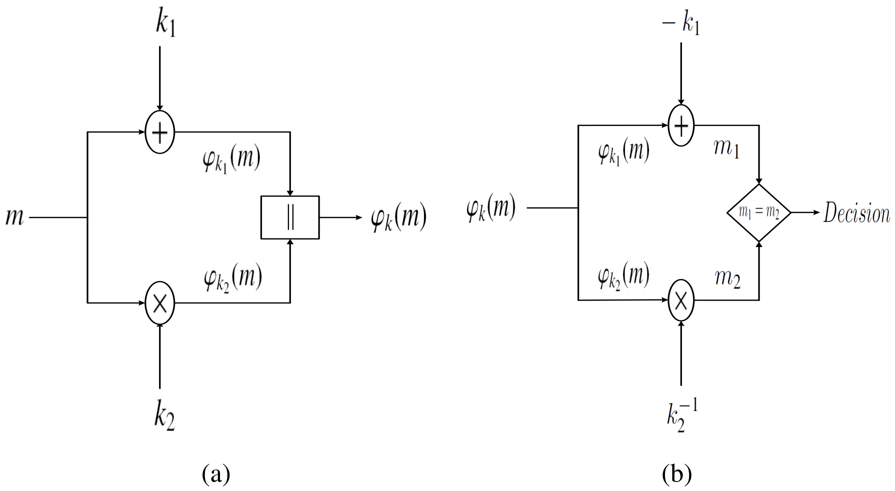

Figure 1: (a) A block diagram to implement the authenticated encryption scheme, and (b) A block diagram implementing the decryption and the validity check of the studied scheme. The addition and multiplication operations are performed over the field $\mathbb{Z}_p$.

4 Security Analysis

In what follows, we prove the security properties of the proposed scheme. Since resilience to active attacks is the main contribution of the our scheme, we will first show that φ_{k_2} serves as a secure MAC for the plaintext m. The security of the MAC is quantified by its resilience to active attacks. More precisely, we will show that if the extracted message, m', passes the integrity check of equation (7), then the probability that $m' \neq m$ is negligible in the security parameter, ℓ, where ℓ is the length of the prime integer, p, in bits.

Theorem 6. *Under Definition 3, the proposed authenticated encryption scheme is resilient to active attacks.*

Proof. There are two cases to be considered here; namely, modifying φ_{k_1} alone, and modifying both φ_{k_1} and φ_{k_2}. Modifying φ_{k_2} alone, since it serves as a MAC, does not lead to extracting a modified plaintext.

Assume that only φ_{k_1} has been modified, maliciously by the adversary or due to channel errors, to φ'_{k_1}. Since k_1 is known to the receiver, this modification will lead to the extraction of an m' that is different than the transmitter's generated m; that is, $m' \equiv \varphi'_{k_1} - k_1 \pmod p$. Let $m' \equiv m + \delta \pmod p$, for some $\delta \in \mathbb{Z}_p \backslash \{0\}$. To be accepted by the receiver, m' must satisfy the following integrity check:

$$
\begin{aligned}
m' \times k_2 &\equiv (m+\delta) \times k_2 \pmod p && (8)\\
&\equiv (m \times k_2) + (\delta \times k_2) \pmod p && (9)\\
&\stackrel{?}{\equiv} \varphi_{k_2} \pmod p && (10)\\
&\equiv m \times k_2 \pmod p. && (11)
\end{aligned}
$$

Lemma 4 guarantees that this modification is detected with probability one. This is due to the fact that the integrity check in equation (10) is satisfied only if equations (9) and (11) are equivalent. Therefore, m' will be accepted as a valid message only if the following condition holds:

$$\delta \times k_2 \equiv 0 \pmod p. \tag{12}$$

However, Lemma 4 states that at least δ or k_2 must be the zero element of $\mathbb{Z}_p$ in order for equation (12) to hold. Since k_2 is chosen from $\mathbb{Z}_p \backslash \{0\}$ and $\delta \not\equiv 0 \pmod p$ by assumption,[2] equation (12) can never be satisfied and, consequently, any modification of φ_{k_1} "alone" will be detected by φ_{k_2} with probability *one*.

We now examine the case where both φ_{k_1} and φ_{k_2} are modified so that a false message will be validated. Assume that φ_{k_1} has been modified so that the extracted message becomes $m' = m+\delta \pmod p$, for some $\delta \in \mathbb{Z}_p \backslash \{0\}$. Also, assume that φ_{k_2} has been modified to $\varphi'_{k_2} = \varphi_{k_2} + \epsilon \pmod p$, for some $\epsilon \in \mathbb{Z}_p \backslash \{0\}$. The integrity of m' is verified using the received φ'_{k_2} as follows:

$$
\begin{aligned}
\varphi_{k_2} + \epsilon &\equiv \varphi'_{k_2} \pmod p && (13)\\
&\stackrel{?}{\equiv} m' \times k_2 \pmod p && (14)\\
&\equiv (m+\delta) \times k_2 \pmod p && (15)\\
&\equiv (m \times k_2) + (\delta \times k_2) \pmod p && (16)\\
&\equiv \varphi_{k_2} + (\delta \times k_2) \pmod p. && (17)
\end{aligned}
$$

By examining equations (13) and (17), the condition for validating the modified m' can be reduced to,

$$\epsilon \equiv \delta \times k_2 \pmod p. \tag{18}$$

Therefore, the adversary's probability of successful forgery becomes:

$$\Pr\Big(\text{successful forgery}\Big) = \Pr\Big(\delta^{-1} \times \epsilon \equiv k_2 \pmod p\Big) \tag{19}$$

If k_2 is known, it is trivial to find two integers δ and ϵ that satisfy equation (18). However, since k_2 is unknown and uniformly distributed over $\mathbb{Z}_p^*$, the adversary's probability of successful forgery by modifying "both" φ_{k_1} and φ_{k_2} is equivalent to randomly guessing the value of k_2, which is equal to $1/(p-1)$.

[2] The value $\delta \equiv 0 \pmod p$ trivially satisfies equation (12); however, it implies that the message has not been modified.

Consequently, since an adversary modifying the ciphertext φ_{k_1} alone will be successful with probability *zero*, and an adversary modifying both ciphertexts φ_{k_1} and φ_{k_2} will be successful with probability $1/(p-1)$, the maximum probability of successful forgery is $1/(p-1)$. Therefore, for an ℓ-bit prime p, the adversary's probability of success is at most $1/2^{\ell-1}$, a negligible function in the security parameter ℓ (according to Definition 2). Therefore, by Definition 3, the proposed scheme is resilient to active attacks. □

Theorem 6 implies that the first requirement of our design, namely message integrity, is satisfied. Observe that not only the proposed scheme is resilient to active attacks, the adversary cannot do better than guessing the value of k_2 to forge a valid MAC, regardless of how much computational power she possesses. Otherwise stated, the integrity of the proposed scheme is unconditionally secure.

The next theorem addresses the second requirement of our design, confidentiality.

Theorem 7. *The proposed scheme achieves perfect secrecy (in Shannon's sense).*

Proof. Let $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ be uniform, independent random variables distributed over $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively. By equation (3), for any given plaintext $m \in \mathbb{Z}_p \backslash \{0\}$, as a result of the uniform distribution of $\boldsymbol{k_1}$ over $\mathbb{Z}_p$, the resulting $\boldsymbol{\varphi_{k_1}}$ is uniformly distributed over $\mathbb{Z}_p$. Similarly, as a result of the uniform distribution of $\boldsymbol{k_2}$ over $\mathbb{Z}_p^*$, by Lemma 5, the resulting $\boldsymbol{\varphi_{k_2}}$ is uniformly distributed over $\mathbb{Z}_p^*$. Consequently, for any arbitrary $\varphi_{k_1} \in \mathbb{Z}_p$ and an arbitrary $\varphi_{k_2} \in \mathbb{Z}_p^*$, the probabilities $\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1})$ and $\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2})$ are $1/p$ and $1/(p-1)$, respectively.

Now, given a specific value of a plaintext message, $\boldsymbol{m} = m$, the probability that the ciphertext $\boldsymbol{\varphi_{k_1}}$ takes a specific value φ_{k_1} is:

$$\begin{aligned}
\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1} | \boldsymbol{m} = m) &= \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m) && (20)\\
&= 1/p && (21)\\
&= \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}). && (22)
\end{aligned}$$

Similarly, given a specific value of a plaintext message, $\boldsymbol{m} = m$, the probability that the ciphertext $\boldsymbol{\varphi_{k_2}}$ takes a specific value φ_{k_2} is:

$$\begin{aligned}
\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2} | \boldsymbol{m} = m) &= \Pr(\boldsymbol{k_2} = \varphi_{k_2} \times m^{-1}) && (23)\\
&= \frac{1}{p-1} && (24)\\
&= \Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2}). && (25)
\end{aligned}$$

Equations (21) and (24) hold since, by design, $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ are uniformly distributed over $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively. The existence of m^{-1}, the multiplicative inverse of the message m modulo p, is a direct consequence of the fact that $m \in \mathbb{Z}_p^*$.

Now, Bayes' theorem, combined with equations (22) and (25), can be used to show that:

$$\Pr(\boldsymbol{m} = m|\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}) = \frac{\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}|\boldsymbol{m} = m)\Pr(\boldsymbol{m} = m)}{\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1})} \tag{26}$$

$$= \Pr(\boldsymbol{m} = m), \tag{27}$$

and

$$\Pr(\boldsymbol{m} = m|\boldsymbol{\varphi_{k_2}} = \varphi_{k_2}) = \frac{\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2}|\boldsymbol{m} = m)\Pr(\boldsymbol{m} = m)}{\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2})} \tag{28}$$

$$= \Pr(\boldsymbol{m} = m). \tag{29}$$

Equations (27) and (29) show that the a posteriori probabilities that the plaintext message is m, given that the observed ciphertexts are φ_{k_1} and φ_{k_2}, are identical to the a priori probability that the plaintext message is m. Hence, both ciphertexts *individually* provide perfect secrecy. However, since they are both an encryption of the same message, there might be information leakage about the plaintext revealed by the combination of φ_{k_1} and φ_{k_2}. One way of measuring how much information is learned by the observation of two quantities is the notion of mutual information. Consider an arbitrary $\varphi_{k_1} \in \mathbb{Z}_p$ and arbitrary $\varphi_{k_2} \in \mathbb{Z}_p^*$. Then, for independent $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ uniformly distributed over $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively, we get:

$$\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}, \boldsymbol{\varphi_{k_2}} = \varphi_{k_2})$$

$$= \sum_m \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}, \boldsymbol{\varphi_{k_2}} = \varphi_{k_2}|\boldsymbol{m} = m)\Pr(\boldsymbol{m} = m) \tag{30}$$

$$= \sum_m \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m, \boldsymbol{k_2} = \varphi_{k_2} \times m^{-1})\Pr(\boldsymbol{m} = m) \tag{31}$$

$$= \sum_m \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m)\Pr(\boldsymbol{k_2} = \varphi_{k_2} \times m^{-1})\Pr(\boldsymbol{m} = m) \tag{32}$$

$$= \sum_m \frac{1}{p} \cdot \frac{1}{p-1}\Pr(\boldsymbol{m} = m) \tag{33}$$

$$= \frac{1}{p} \cdot \frac{1}{p-1} \tag{34}$$

$$= \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1})\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2}). \tag{35}$$

Equation (32) holds due to the independence of $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$, equation (33) holds due to the uniform distribution of $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$, and equation (35) holds due to the uniform distribution of $\boldsymbol{\varphi_{k_1}}$ and $\boldsymbol{\varphi_{k_2}}$. Consequently, $\boldsymbol{\varphi_{k_1}}$ and $\boldsymbol{\varphi_{k_2}}$ are independent and, thus, their mutual information is [Cover and Thomas(2006)]:

$$I(\boldsymbol{\varphi_{k_1}}; \boldsymbol{\varphi_{k_2}}) = \sum_{\varphi_{k_1}} \sum_{\varphi_{k_2}} \Pr(\varphi_{k_1}, \varphi_{k_2}) \log\left(\frac{\Pr(\varphi_{k_1}, \varphi_{k_2})}{\Pr(\varphi_{k_1})\Pr(\varphi_{k_2})}\right) = 0. \tag{36}$$

Therefore, observing both ciphertexts, φ_{k_1} and φ_{k_2}, gives no extra information about the plaintext than what the ciphertexts φ_{k_1} and φ_{k_2} give individually.

By definition of one-time pad ciphers, the keys $k = k_1||k_2$ and $k' = k'_1||k'_2$ used for two different encryption operations must be random and independent. Thus, the independence of the two ciphertexts follows directly from the independence of the keys. For example, let φ_{k_1} and φ'_{k_1} represent the encryption of message m with two independent keys k_1 and k'_1, respectively. Then,

$$\begin{aligned}
&\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}, \boldsymbol{\varphi'_{k_1}} = \varphi'_{k_1}) \\
&\qquad = \sum_m \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}, \boldsymbol{\varphi'_{k_1}} = \varphi'_{k_1} | \boldsymbol{m} = m) \Pr(\boldsymbol{m} = m) && (37)\\
&\qquad = \sum_m \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m, \boldsymbol{k'_1} = \varphi'_{k_1} - m) \Pr(\boldsymbol{m} = m) && (38)\\
&\qquad = \sum_m \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m) \Pr(\boldsymbol{k'_1} = \varphi'_{k_1} - m) \Pr(\boldsymbol{m} = m) && (39)\\
&\qquad = \frac{1}{p} \cdot \frac{1}{p} && (40)\\
&\qquad = \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}) \Pr(\boldsymbol{\varphi'_{k_1}} = \varphi'_{k_1}), && (41)
\end{aligned}$$

where equation (39) holds due to the independence of $\boldsymbol{k_1}$ and $\boldsymbol{k'_1}$. Hence, $\boldsymbol{\varphi_{k_1}}$ and $\boldsymbol{\varphi'_{k_1}}$ are independent. Similarly, $\boldsymbol{\varphi_{k_i}}$ and $\boldsymbol{\varphi'_{k_i}}$ for $i = 1, 2$ can shown to be mutually independent, leading to the independence of $\boldsymbol{\varphi_k}$ and $\boldsymbol{\varphi'_k}$. Thus, no information about plaintext messages can be obtained by observing their corresponding ciphertexts, provided that the keys used for different encryptions are independent and random. Therefore, the described cipher is indeed information-theoretically secure. □

So far, we have shown that φ_{k_2}, using a single modular multiplication, serves as unconditionally secure MAC of the encrypted message, m, without affecting its perfect secrecy. The next section is devoted to comparing the proposed scheme to existing approaches that can achieve the same goals, and to discussing some potential applications where the proposed scheme can be useful.

5 Discussions and Applicability

5.1 Comparison

Consider the classic use of universal hash families for unconditionally secure message authentication. Given a secret key, $(a, b) \in \mathbb{Z}_p^2$, a message, m, is authenticated by the code,

$$MAC(m) = am + b \pmod{p}. \tag{42}$$

That is, unconditionally secure integrity is accomplished with two keys, a and b, and two modular operations in $\mathbb{Z}_p$, one addition and one multiplication. With the same two keys and the same two operations, the proposed scheme can achieve the same level of message integrity, *in addition to perfect secrecy*. In other words, our scheme provides additional perfect secrecy with absolutely no extra key material and no extra computational effort.

To get the same level of message secrecy and integrity, without using the proposed scheme, one will need to encrypt the message with a one-time key, then implement the encrypt-then-authenticate approach with an unconditionally secure MAC to authenticate the ciphertext. Therefore, one will need three keys, one for encryption and two for authentication, in addition to computing one modular multiplication and two modular addition. Therefore, the proposed scheme can achieve the same security goals with less key material and fewer computations. That is, instead of two keys for authentication, one key can be used to achieve the same level of integrity. Since key length requirement is the most important issue in one-time pad systems, a 50% reduction on key length requirement, for the same security results using less computational effort, is a considerable improvement. A further substantial key reduction is described in Section 6.

The new idea introduced here is to combine encryption and authentication using one-time key to achieve both perfect secrecy and unconditional message integrity in one round. By taking advantage of the fact that the message to be authenticated is secret, properties of the integer filed $\mathbb{Z}_p$ are used to authenticate the message with a single key using one multiplication operation. This idea of authenticating secret messages using a single modular multiplication has appeared the first time in [Aloamir and Poovendran(2009)].

Moreover, recall that, by Theorem 6, any modification of only one of φ_{k_1} or φ_{k_2} will be detected with probability one. If the sender has the ability to transmit the encryption, φ_{k_1}, and the authentication tag, φ_{k_2}, over two different channels, at which the adversary controls only one of them, message integrity is guaranteed with probability *one*. This includes applications where the adversary is equipped with only one antenna, and applications where frequency hopping techniques are used for transmission at which the adversary does not detect both channels. With the increase spreading of frequency hopping techniques in the context of providing security for a variety of applications in wireless communications (see, e.g., [Strasser et al.(2008)Strasser, Popper, Capkun and Cagalj]), the proposed idea might be useful for providing a strong notion of message integrity in some applications.

5.2 Potential Applications

Even though one-time pad ciphers are believed to be impractical in many situations due to their key requirement, they might be desirable in exchanging highly confidential diplomatic or military information. In fact, the hotline between Moscow and Washington D.C., established in 1963 after the Cuban missile crisis, used teleprinters protected by a commercial one-time tape system. Each country prepared the keying tapes used to encode its messages and delivered them via their embassy in the other country [Kahn(1974)]. Given the simplicity and high level of integrity of the proposed scheme, we believe it is a very suitable method to provide integrity to OTP ciphers in cases where both unconditional secrecy and integrity are desired.

In a totally different direction, consider a scenario where a businessman is in a trip and needs to send an urgent confidential message to his broker (e.g.,"buy 1,000,000 shares"). In addition to authenticity, the confidentiality of this message might be of extreme importance to the businessman. Given the simple computations of the proposed scheme (single addition and multiplication), the task can be accomplished, with unconditional secrecy and integrity, using a basic calculator (or even by hand). If the businessman is equipped with a mobile device that can store few megabytes of data (for the secret key), he can implement the proposed technique to transmit multiple authenticated encrypted messages before exhausting his key, without the need to carry sophisticated devices.

In another application, consider a battery powered, computationally constrained sensor node that is setup to send updated measurements to its anchor node every hour. Assuming each measurement is 20-byte long, and the node is preloaded with only one megabyte long secret key. The node can use the proposed scheme to send unconditionally secure measurements in a perfectly secret manner, with probability of validating a corrupted measurement less than 1.4×10^{-48},[3] for about three years before it exhausts its preloaded secret key. On the other hand, if the existing method of encrypting with one-time keys followed by authenticating using universal hash families, as described earlier, the lifetime of the system will be reduced to bout two years. Furthermore, the reduction in key usage detailed in the next section can almost double the lifetime of the system.

In summary, this method can be applicable to provide the highest level of information secrecy and integrity for pairwise communications. Considering the relatively cheap price for storage devices in today's technology, users can exchange large amounts of keying information, out of band, and use them for a sufficiently long time to secure their pairwise communications.

6 Almost Free Authentication

In this section, we discuss a modification of the proposed scheme that can substantially reduce the length of the authentication key, k_2, in the proposed scheme.

Let the message to be encrypted be $m \in \mathbb{Z}_{2^n} \backslash p\mathbb{Z}$ (as opposed to $m \in \mathbb{Z}_p \backslash \{0\}$ as in the original scheme), for an arbitrary message length, n. Further, let n (the length of the message in bits) be greater than ℓ (the length of p in bits). Then, for $k_1 \in \mathbb{Z}_{2^n}$ and $k_2 \in \mathbb{Z}_p^*$, define two functions $\varphi_{k_1}(m) : \mathbb{Z}_{2^n} \backslash p\mathbb{Z} \rightarrow \mathbb{Z}_{2^n}$ and $\varphi_{k_2}(m) : \mathbb{Z}_{2^n} \backslash p\mathbb{Z} \rightarrow \mathbb{Z}_p^*$

[3] Assuming ℓ is also 20-byte long.

as follows:

$$\varphi_{k_1}(m) \equiv k_1 + m \pmod{2^n}, \tag{43}$$

$$\varphi_{k_2}(m) \equiv k_2 \times m \pmod{p}. \tag{44}$$

As before, the ciphertext is the concatenation of $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$. The obvious problem here is that all messages that are different by multiples of p will be mapped to the same $\varphi_{k_2}(m)$ and, unlike the original scheme where $m \in \mathbb{Z}_p^*$, that does not imply that the messages are the same. That is, since $m \in \mathbb{Z}_{2^n} \backslash p\mathbb{Z}$, $m \pm p\mathbb{Z} \not\equiv m \pmod{2^n}$, while $\varphi_{k_2}(m \pm p\mathbb{Z}) \equiv \varphi_{k_2}(m) \pmod{p}$. Therefore, any modification of the message by multiples of p will go undetected, leading to the acceptance of modified messages. Next, we describe our solution to this problem.

6.1 Unknown Modulus

Recall that, by equation (12), an adversary modifying $\varphi_{k_1}(m)$ alone is undetected if and only if

$$\delta \times k_2 \equiv 0 \pmod{p}, \tag{45}$$

for some $\delta \in \mathbb{Z}_{2^n} \backslash \{0\}$ of the adversary's choice. Furthermore, by equation (19), an adversary modifying both $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$ is undetected if and only if

$$\delta^{-1} \times \epsilon \equiv k_2 \pmod{p}, \tag{46}$$

for some non-zero δ and ϵ of the adversary's choice.

Therefore, if the prime modulus, p, is unknown to the adversary, then the probability of successful forgery by modifying $\varphi_{k_1}(m)$ alone is equivalent to guessing the prime p. This is because only if $\delta \in p\mathbb{Z}$ it will satisfy equation (45). Now, even if the adversary is assumed to know the length of the prime integer, say ℓ-bits, the prime number theorem shows that the number of primes less than 2^ℓ can be approximated by [Cormen et al.(1999)Cormen, Leiserson and Rivest]:

$$\pi(2^\ell) \approx 2^\ell / \ell \ln(2), \tag{47}$$

where $\pi(x)$ is the prime-counting function. That is, the probability of randomly guessing the used prime integer is an exponentially decreasing function in ℓ. (The adversary can also increase her chances by multiplying multiple ℓ-bit primes, but devices will overflow rather quickly. For example, using MATLAB 2007, multiplying 10 primes of length 100-bits caused an overflow.)

On the other hand, solving equation (46) is still equivalent to guessing the value of k_2. Hence, the probability of successful forgery by modifying both $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$ is still $1/(p-1)$, as in the original scheme. Therefore, the probability of successful forgery, in the modified scheme, is a negligible function in the security parameter and, thus, the modified scheme is also resilient to active attacks.

However, for security reasons, it is impractical in cryptographic literature to assume that the used modulus, p, will remain secret.[4] To overcome this problem, we propose below a method to secretly exchange a new prime modulus (to be used for authentication) for each operation.

6.2 Exchanging the Modulus Secretly

Assume that the prime modulus, p, has not been agreed-upon and is unknown to the intended receiver. Given the length of φ_{k_1}, say n bits, the receiver uses n bits of secret key material to construct k_1. By subtracting the constructed k_1 from the received φ_{k_1} modulo 2^n (or alternatively XORing k_1 with φ_{k_1} if the XOR operation is used for encryption), the receiver can correctly decrypt the transmitted message. Assuming that p is embedded somewhere in the encrypted message, the receiver can extract it and use it for authentication. Since the message is sent in a perfectly secret manner, the adversary can do no better than randomly guessing the value of p.

With this described approach, the authentication key, k_2, can be much shorter than the length of the message. For example, a 128-bit key can be used to authenticate an arbitrarily long message with high level of integrity. Therefore, this approach can substantially reduce the amount of required key material.

7 Authenticating Short Encrypted Messages

In this section we deviate from unconditionally secure authentication and describe a method that exploits the fact that the message to be authenticated is encrypted so that it can be authenticated with a single multiplication. This method can be very efficient when the message to be authenticated is short. In traditional MACs, due to the fact that messages to be authenticated are usually required to have certain lengths, special attention must be paid to authenticating short messages. Therefore, traditional message authentication codes can be inefficient when the message to be authenticated is short. For example, UMAC, the fastest reported message authentication code in the cryptographic literature [van Tilborg(2005), Krovetz(2006)], has undergone large algorithmic changes to increase its speed on short messages.

Consider now a short messages that is to be encrypted with any semantically secure encryption scheme. Instead of authenticating the message using a traditional MAC, consider the following procedure. Let the sender generate a fresh random key k_a and a prime number p and append them to the message before encryption. That is, the plaintext to be encrypted becomes $(m \parallel k_a \parallel p)$, where "$\parallel$" denotes the concatenation operation. The sender then can authenticate the message m using the same method

[4] An adversary, for instance, can infer a lower bound on the used modulus by the observation of an authentication tag. This lower bound can only get tighter as the number of observed tags increases.

described in Section 6. That is, the sender can compute an authentication tag as follows:

$$\sigma = m \times k_a \pmod{p}. \tag{48}$$

Upon receiving the ciphertext, the intended receiver can decrypt the message and extract m, k_a, and p. Given σ, the receiver can check the validity of the message as follows:

$$\sigma \stackrel{?}{\equiv} m \times k_a \pmod{p}. \tag{49}$$

Obviously, the authentication tag must satisfy two requirements: first, it must provide the required integrity and, second, it must not jeopardize the secrecy of the encrypted message. The following two theorems show that the authentication tag satisfies both requirements.

Theorem 8. *An adversary forging valid tags with a non negligible probability is able to break the encryption scheme.*

Proof. By Lemma 5, the tag is uniformly distributed over $\mathbb{Z}_p^*$. Therefore, given that both k_a and m are unknown, the adversary cannot forge a valid tag with a non negligible probability. That is, for an adversary to have a non negligible probability of successful forgery, she has to know the secret values of m, k_a, and p. In other words, the adversary will need to break the encryption scheme to be able to forge valid tags. □

Theorem 9. *An adversary exposing information about the encrypted message from the authentication tag is able to break the encryption scheme.*

Proof. If the key k_a is delivered to the receiver out of band, equation (48) can be viewed as an encryption of the plaintext message m with a perfectly secret one-time pad cipher. Similarly, given the semantic security of the underlying encryption algorithm, the adversary cannot infer any information about the encrypted key k_a. Therefore, unless the adversary can break the encryption algorithm to learn secret information about k_a, no information about the plaintext message m can be exposed by its authentication tag.

□

Theorems 8 and 9 imply that breaking the security of the authentication tag is reduced to breaking the underlying encryption scheme. That is, the proposed method is provably secure, given the semantic security of the underlying encryption algorithm.

8 Conclusion

In this work, the problem of authenticated encryption is addressed. Three schemes were proposed. In the first scheme, an OTP cipher that carries its own MAC in a way that preserves perfect secrecy is proposed. The proposed scheme utilizes the fact that the message to be authenticated is encrypted to achieve unconditionally secure authentication with half the key material required by traditional unconditionally secure authentication. Then we proposed an extension to the first scheme that exploits further the fact that the message to be authenticated is encrypted to authenticate it with almost no extra key material. The idea behind the extended scheme is to pass a prime number, that is much shorter than the message to be authenticated, in a perfectly secret manner. The prime number can be used as an unknown modulus to authenticate the message by multiplying it with a shared key. Finally, we deviated from unconditionally secure authentication to propose a provably secure message authentication. Again, the scheme takes advantage of the fact that the message to be authenticated is encrypted with a semantically secure encryption scheme to pass a random key along with the message. This random key is used to authenticate the encrypted message using a single multiplication operation. The significant of this scheme is that it allows for a very efficient message authentication in scenarios where the message to be authenticated is short.

References

[Aloamir and Poovendran(2009)] Aloamir, B., Poovendran, R.: "Unconditionally Secure Authenticated Encryption with Shorter Keys"; The 7th International Workshop on Security in Information Systems–WOSIS'09; (2009).

[Bellare et al.(1996)Bellare, Canetti and Krawczyk] Bellare, M., Canetti, R., Krawczyk, H.: "Keying hash functions for message authentication"; Advances in Cryptology–CRYPTO; 96 (1996), 1–15.

[Bellare et al.(1995)Bellare, Guerin and Rogaway] Bellare, M., Guerin, R., Rogaway, P.: "XOR MACs: New methods for message authentication using finite pseudorandom functions"; Advances in Cryptology–CRYPTO95 (LNCS 963); (1995), 15–28.

[Bellare and Namprempre(2000)] Bellare, M., Namprempre, C.: "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm"; Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology–ASIACRYPT; (2000), 531–545.

[Bellare et al.(2004)Bellare, Rogaway and Wagner] Bellare, M., Rogaway, P., Wagner, D.: "The EAX mode of operation"; Fast Software Encryption; (2004), 389–407.

[Bernstein(2005)] Bernstein, D.: "The Poly1305-AES message-authentication code"; Proceedings of FSE; 32–49; Springer, 2005.

[Black et al.(1999)Black, Halevi, Krawczyk, Krovetz and Rogaway] Black, J., Halevi, S., Krawczyk, H., Krovetz, T., Rogaway, P.: "UMAC: Fast and Secure Message Authentication"; Advances in Cryptology-Crypto'99: 19th Annual International Cryptology Conference, Santa Barbara, California, USA August 15-19, 1999 Proceedings; (1999).

[Cormen et al.(1999)Cormen, Leiserson and Rivest] Cormen, T., Leiserson, C., Rivest, R.: Introduction to Algorithms; McGraw-Hill, 1999.

[Cover and Thomas(2006)] Cover, T., Thomas, J.: Elements of Information Theory; Wiley-Interscience New York, 2006.

[Elgamal(1985)] Elgamal, T.: "A public key cryptosystem and a signature scheme based on discrete logarithms"; Information Theory, IEEE Transactions on; 31 (1985), 4, 469–472.

[Etzel et al.(1999)Etzel, Patel and Ramzan] Etzel, M., Patel, S., Ramzan, Z.: "Square hash: Fast message authentication via optimized universal hash functions"; Lecture Notes in Computer Science; (1999), 234–251.

[Ferguson et al.(2003)Ferguson, Whiting, Schneier, Kelsey, Lucks and Kohno] Ferguson, N., Whiting, D., Schneier, B., Kelsey, J., Lucks, S., Kohno, T.: "Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive, Fast Software Encryption 2003, LNCS 2887"; (2003).

[Freier et al.(1996)Freier, Karlton and Kocher] Freier, A., Karlton, P., Kocher, P.: "The SSL Protocol Version 3.0"; (1996).

[Gilbert et al.(1974)Gilbert, MacWilliams and Sloane] Gilbert, E., MacWilliams, F., Sloane, N.: "Codes which detect deception"; Bell System Technical Journal; 53 (1974), 3, 405–424.

[Gligor and Donescu(2000)] Gligor, V., Donescu, P.: "Integrity-Aware PCBC Encryption Schemes"; Security Protocols: 7th International Workshop, Cambridge, Uk, April 19-21, 1999: Proceedings; (2000).

[Gligor and Donescu(2002)] Gligor, V., Donescu, P.: "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes"; Fast Software Encryption: 8th International Workshop, FSE 2001, Yokohama, Japan, April 2-4, 2001: Revised Papers; (2002).

[Goldreich(2001)] Goldreich, O.: Foundations of Cryptography; Cambridge University Press, 2001.

[Halevi and Krawczyk(1997)] Halevi, S., Krawczyk, H.: "MMH: Software message authentication in the Gbit/second rates"; Lecture notes in computer science; (1997), 172–189.

[Jutla(2001)] Jutla, C.: "Encryption modes with almost free message integrity"; Advances in Cryptology–EUROCRYPT; 2045 (2001), 529–544.

[Kahn(1974)] Kahn, D.: The codebreakers; Weidenfeld and Nicolson, 1974.

[Kaps et al.(2005)Kaps, Yuksel and Sunar] Kaps, J., Yuksel, K., Sunar, B.: "Energy scalable universal hashing"; IEEE Transactions on Computers; 54 (2005), 12, 1484–1495.

[Kent(2005)] Kent, S.: "RFC4303: IP encapsulating security payload (ESP),"; Internet EFC. STD. FYI/BCP archives. December; (2005).

[Kohl and Neuman(1993)] Kohl, J., Neuman, C.: "The Kerberos Network Authentication Service (V5)"; Technical report; RFC 1510, September 1993 (1993).

[Kohno et al.(2004)Kohno, Viega and Whiting] Kohno, T., Viega, J., Whiting, D.: "CWC: A high-performance conventional authenticated encryption mode"; Fast Software Encryption; (2004), 408–426.

[Krawczyk(2001)] Krawczyk, H.: "The order of encryption and authentication for protecting communications(or: How secure is SSL?)"; Advances in Cryptology–CRYPTO 2001; (2001), 310–331.

[Krovetz(2006)] Krovetz, T.: (2006).

[McGrew and Viega(2004)] McGrew, D., Viega, J.: "The security and performance of the Galois/Counter Mode (GCM) of operation"; Progress in Cryptology-INDOCRYPT; (2004), 343–355.

[Meyer and Matyas(1982)] Meyer, C., Matyas, S.: Cryptography: A New Dimension in Computer Data Security; John Wiley & Sons, 1982.

[Rogaway et al.(2003)Rogaway, Bellare and Black] Rogaway, P., Bellare, M., Black, J.: "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption"; ACM Trans. Inf. Syst. Secur.; 6 (2003), 3, 365–403.

[Rogaway and Black(2001)] Rogaway, P., Black, J.: "PMAC: Proposal to NIST for a parallelizable message authentication code"; (2001).

[Shannon(1949)] Shannon, C.: Communication Theory and Secrecy Systems; Bell Telephone Laboratories, 1949.

[Simmons(1988)] Simmons, G.: "A Survey of Information Authentication"; Proceedings of the IEEE; 76 (1988), 5, 603–620.

[Stinson(1994)] Stinson, D.: "Universal Hashing and Authentication Codes"; Designs, Codes and Cryptography; 4 (1994), 3, 369–380.

[Stinson(1996)] Stinson, D.: "On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes"; Congressus Numerantium; (1996), 7–28.

[Stinson(2006)] Stinson, D.: Cryptography: Theory and Practice; CRC Press, 2006.

[Strasser et al.(2008)Strasser, Popper, Capkun and Cagalj] Strasser, M., Popper, C., Capkun, S., Cagalj, M.: "Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping"; IEEE Symposium on Security and Privacy, 2008. SP 2008.; 64–78; 2008.

[US National Bureau of Standards(December 1980)] US National Bureau of Standards: "DES Modes of Operation"; Federal Information Processing Standard (FIPS) Publication 81; Available as http://www.itl.nist.gov/fipspubs/fip81.htm (December 1980).

[van Tilborg(2005)] van Tilborg, H.: Encyclopedia of cryptography and security; Springer, 2005.

[Vernam(1926)] Vernam, G.: "Cipher printing telegraph systems for secret wire and radio telegraphic communications"; Journal of the American Institute of Electrical Engineers; 45 (1926), 109–115.

[Wegman and Carter(1979)] Wegman, M., Carter, J.: "New classes and applications of hash functions"; Foundations of Computer Science, 1979., 20th Annual Symposium on; (1979), 175–182.

[Wegman and Carter(1981)] Wegman, M., Carter, L.: "New hash functions and their use in authentication and set equality"; J. Comput. Syst. Sci.; 22 (1981), 3, 265–279.

[Ylonen and Lonvick(2006)] Ylonen, T., Lonvick, C.: "The Secure Shell (SSH) Transport Layer Protocol"; Technical report; RFC 4253, January 2006 (2006).